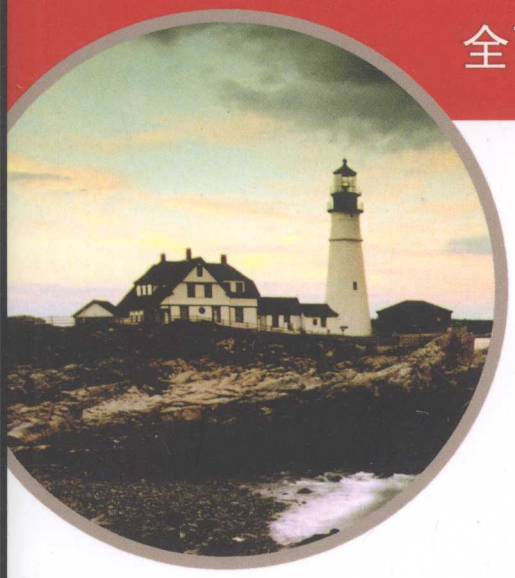
全面、透彻讲解CISSP考试全部考点



本书提供包括多个真实场景，提供丰富的习题，还配备了光盘。光盘中的前沿备考软件包含：

- 自定义测验引擎
- PDF格式的英文版电子书
- 两套包含250道题的标准模拟试题
- 可以运行在PC、掌上电脑或Palm掌上设备上的用于辅助记忆的电子抽认卡

CISSP: Certified Information Systems Security Professional Study Guide Fourth Edition

CISSP

认证考试权威指南

(第4版)

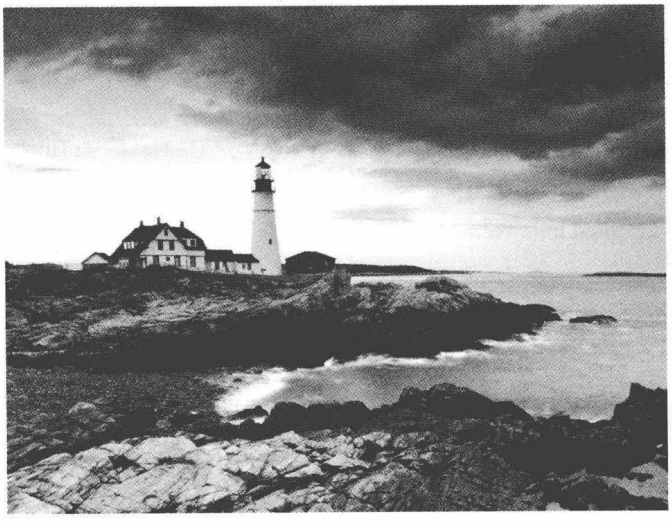
James Michael Stewart
(美) Ed Tittel 著
Mike Chapple
梁志敏 译

SYBEX

清华大学出版社

CISSP 认证考试权威指南

(第 4 版)



James Michael Stewart
(美) Ed Tittel 著
Mike Chapple
梁志敏 译

清华大学出版社
北 京

James Michael Stewart, Ed Tittel, Mike Chapple
CISSP: Certified Information Systems Security Professional Study Guide Fourth Edition
EISBN：978-0-470-27688-4

北京市版权局著作权合同登记号 图字：01-2009-2536

图书在版编目(CIP)数据

CISSP 认证考试权威指南(第 4 版)/ (美) 迈克尔(Michael，J.)，(美) 泰特尔(Tittel，E.)，(美) 查佩尔(Chapple，M.) 著；梁志敏 译. —北京：清华大学出版社，2010.1

书名原文：CISSP: Certified Information Systems Securiy Profesional Study Guide Fourth Edition

ISBN 978-7-302-21537-0

Ⅰ. ①C…　Ⅱ. ①迈…　②泰…　③查…　④梁…　Ⅲ. ①信息系统－安全技术－资格考核－自学参考资料　Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字(2009)第 218570 号

责任编辑：王　军　韩宏志
装帧设计：孔祥丰
责任校对：成凤进
责任印制：孟凡玉
出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　　编**：100084
社　总　机：010-62770175　　**邮　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：清华大学印刷厂
装 订 者：三河市新茂装订有限公司
经　　销：全国新华书店
开　　本：185×260　**印　张**：42　**字　数**：1022 千字
附光盘 1 张
版　　次：2010 年 1 月第 1 版　　**印　　次**：2010 年 1 月第1 次印刷
印　　数：1～4000
定　　价：89.00 元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。联系电话：(010)62770177 转 3103　　产品编号：030089-01

作 者 简 介

James Michael Stewart，信息系统安全认证专家，从事写作与培训工作已有 14 年之久，其作品始终与最新的安全热点相结合。他教授许多 CISSP 培训课程，此外，还参加众多与 Windows 安全性和 Certified Ethical Hacker 认证相关的会议。Michael 的一些著作和教材主要涉及安全认证、Microsoft 专题以及网络管理。读者可以在其 Web 站点 www.impactonline.com 上了解到 Michael 的更多信息。

Ed Tittel，从事自由职业的作家、培训师和顾问，精通信息安全、标记语言与网络连接技术的相关知识。他是许多 TechTarget 站点的定期撰稿人；与 HP、Sony 和 Motorola 等许多公司合作，讲授联机安全和技术课程；并且定期为 Tom's Hardware 站点提供稿件。读者可以在其 Web 站点 www.edtittel.com 上了解到 Ed 的更多信息。

Mike Chapple，信息系统安全认证专家，Notre Dame 大学的 IT 安全专家。曾任 Brand Institute 的首席信息主管以及美国国家安全局和美国空军的信息安全研究员。Mike 的主要专业领域包括网络入侵检测和访问控制，他是 TechTarget SearchSecurity 站点的长期撰稿人，*Information Security* 杂志的技术编辑。Mike 编著了一些与信息安全相关的著作，包括 Wiley 出版社发行的 *The GSEC Prep Guide* 以及 Jones and Bartlett Publishers 出版社发行的 *Information Security Illuminated*。

前　言

本书为读者提供了信息系统安全专家认证(Certified Information Systems Security Professional，CISSP)考试的完备基础知识。购买本书表示你愿意学习和进一步了解 CISSP 考试要求掌握的技能。本部分概述了本书与 CISSP 考试的内容。

本书是专门为参加 CISSP 认证考试的读者和学生编写的。如果你有志成为一名通过认证的安全专家，那么 CISSP 认证和这本学习指南就非常适合你。本书的目的就是要帮助你为通过 CISSP 认证考试做好充分的准备。

在开始阅读本书之前，你需要先独自完成一些工作。你应当对 IT 及安全性有大致的了解，应当在 CISSP 考试所覆盖十个领域中的某个领域具有 5 年的工作经历(或 4 年的工作经历加上大学学位)。根据$(ISC)^2$，如果你具有参加 CISSP 考试的资格，那么可以使用本书充分地准备 CISSP 考试。接下来将介绍有关$(ISC)^2$的更多信息。

$(ISC)^2$

CISSP 考试由国际信息系统安全认证协会(International Information Systems Security Certification Consortium，$(ISC)^2$)管理。$(ISC)^2$ 是一个全球性的非赢利性组织，该组织具有四个主要的目标：

- 为信息系统安全领域维护公共知识体系(Common Body of Knowledge，CBK)。
- 为信息系统安全专业人士和从业人员提供认证。
- 指导认证培训和管理认证考试。
- 通过连续的教育培训，对有资格的认证候选人的鉴定工作进行管理。

$(ISC)^2$ 由董事会运作，董事会成员从通过认证的从业人员中按级别选举产生。要了解$(ISC)^2$的更多信息，可以访问其 Web 站点 www.isc2.org。

CISSP 与 SSCP

$(ISC)^2$ 支持并提供两种主要的认证考试：CISSP 和 SSCP。这些认证考试用于证实所有行业的 IT 安全专业人士的知识与技能。CISSP 考试针对的是组织机构内负责设计和维护安全基础结构的安全专业人士；系统安全从业人员认证(System Security Certified Practitioner，SSCP)考试针对的则是组织机构内负责实现或运作安全基础结构的安全专业人士。

CISSP 认证考试涵盖了 CBK10 个领域的知识：

- 访问控制

- 电信与网络安全
- 信息安全与风险管理
- 应用安全
- 密码术
- 安全体系结构与设计
- 操作安全
- 业务连续性与灾难恢复计划
- 法律、合规性与调查
- 物理(环境)安全

SSCP 认证考试涵盖了 CBK7 个领域的知识：

- 访问控制
- 管理
- 审计与监控
- 密码术
- 数据通信
- 恶意代码/恶意软件
- 风险、响应与恢复

虽然 CISSP 和 SSCP 认证考试内容所涉及的领域有重复之处，但是它们各自具有不同的侧重点。CISSP 主要关注于理论和设计，而 SSCP 则更关注实现与最佳方法。本书的重点只集中在 CISSP 考试所涉及的领域。

资格预审

$(ISC)^2$ 定义了成为一名 CISSP 所必须满足的几项资格。首先，你必须具有至少 5 年的安全从业经历，或者具有至少 4 年的安全从业经历加上近期的 IT 或 IS 学位。专业经历的定义是：在 CBK 十个领域中的一个或多个领域从事有工资收入的安全工作。

其次，你必须认可遵守相关的道德规范。CISSP 的道德规范是$(ISC)^2$希望所有 CISSP 候选人都要遵守的一套准则，其目的是为了维护信息系统安全领域的职业道德。你可以在$(ISC)^2$的 Web 站点 www.isc2.org 的 Information 部分中找到这些准则。

$(ISC)^2$还提供了一个被称为 Associate of $(ISC)^2$的报名程序，这个程序允许由于没有安全从业经历或从业经历不足而未获得 CISSP 资格的任何人都能够先参加 CISSP 考试，随后再获取所要求的经历。Associate of $(ISC)^2$的资格能够保留 6 年，以便相关人员获得 5 年的安全从业经历。只有在提供安全从业证明(通常采用提交书面证明和简历的方式)之后，$(ISC)^2$才会为其授予 CISSP 认证证明。

要想报名参加 CISSP 考试，请访问$(ISC)^2$的 Web 站点，并且按照指导(即链接“Register Now for CISSP Certification Exams”)完成参加 CISSP 考试的注册。你需要提供自己的联系方式、付款信息以及有关安全行业的专业经历，并且还要选择可以参加考试的时间和地点。一旦$(ISC)^2$批准了参加考试的申请，你就会收到一封确认邮件，这封邮件提供了有关考试中心与参加考试的详细信息。

CISSP 考试概述

CISSP 考试由 250 个问题组成，考试用时 6 个小时。考生参加考试时仍旧使用一本小册子和答案纸，也就是说需要使用铅笔来填写答案框。

CISSP 考试从较深的层次关注安全，它更注重理论和概念，而不是关注实现与过程。考试所涉及的范围非常广，但较为浅显。为了成功通过 CISSP 考试，你需要熟悉 CBK 中的所有领域，不过没有必要成为每个领域的专家。

你需要通过(ISC)^2 的 Web 站点 www.isc2.org 进行考试注册。

(ISC)^2 全权管理 CISSP 考试。在大多数情况下，考试在酒店的大会议室内进行。CISSP 资格的现有所有者被聘用为考试的监考人或管理人。请务必在早上 8:00 左右到达考试中心。需要牢记的是，早上 8:30 以后禁止任何考生进入考场。一旦所有参考人员签到就坐，监考人就会发放考试小册子并宣读一些注意事项，这至少需要 30 分钟的时间。随后，长达 6 小时的考试将正式开始。

CISSP 考试的题型

CISSP 考试的每一道题都有 4 个选项，但是其中只有一个选项是正确答案。有些问题非常简单，如选择正确的定义；有些问题较为复杂，如选择适当的概念或最优方法；另外一些问题则描述某个场景或环境，考生需要选择最佳的解决方案。下面给出了一道例题：

1. What is the most important goal and top priority of a security solution?

A. Preventing disclosure　　B. Maintaining integrity

C. Maintaining human safety　　D. Sustaining availability

你必须选择一个正确的或是最合适的答案，并且标记在答案纸上。某些情况下，正确答案显而易见。另外一些情况下，可能会有几个答案看上去都是正确的；遇到这种情况时，你必须选择最适合这道问题的答案。考试时，一定要留意那些一般性的、明确的、全面的、扩展集和子集选项。如果在某些情况下，似乎没有一个答案是正确的，那么你就要选择错误可能性最小的答案。

此例题的答案为 C。保护人员安全应当始终是首先考虑的问题。

答题建议

参加 CISSP 考试时有两个关键要素。首先，必须了解 CBK 十个领域所涉及的内容。其次，一定要具有良好的考试技巧。要想在 6 个小时内完成 250 个问题的考试，每道题的平均答题时间不能超过 90 秒。因此，快速答题十分重要，虽然考生不能过于仓促，但也不能拖拖拉拉，浪费时间。

需要记住的一个关键因素是，猜测答案总比不回答问题强。如果你跳过某个问题，那

么该题将不得分。但是，如果猜测一个答案，那么你至少有 25%的机会得分。答案错误并不扣分，对你来说也不会造成任何损失。因此，在 6 个小时的考试时间即将结束之前，请确认答题纸上的每道题都标记了答案。

你可以在考试小册子上写字，但是写在上面的任何东西都不会用来计算得分。你可以使用小册子作笔记与掌握考试进度。我们建议你在将答案标记到答案纸上之前，再仔细看一下所选择的每一个答案。

为了激发你参加考试的最大潜能，下面给出了一些一般性的指导原则：

- 首先回答简单的问题。
- 跳过较难的问题，稍后再返回思考。为了记住被跳过的问题，可以在考试小册子的封面上记下它们的题号。
- 在选择正确的答案之前，先排除错误的答案。
- 注意双重否定的问题。
- 务必了解问题的含义。

合理安排考试时间。你应当在一个小时内完成大约 50 个问题，这样才能在留下的一个小时内重新考虑被跳过的问题并重新检查一遍。

一定格外注意要把答案标记在答案纸上的正确题号下。考生最容易犯的错误是：考试小册子上的题号与答题纸上的题号顺序发生了错位。

记着携带食物和饮料进入考场。考试期间，考生不得离开考场就餐。考生的食物与饮料存放在考场靠墙处。你可以随时补充食物和饮料，但是只能在墙壁旁边进行。还应当携带药品或其他必要的物品，但是所有电子用品都严禁带入考场。考生可以戴手表，但是绝对不能使用可编程的手表。此外，还需携带铅笔、人工刨笔刀以及橡皮擦。

如果英语不是你的母语或第一外语，那么可以注册使用 CISSP 考试允许的某种语言。否则，如果选择使用英语参加考试，你可以携带翻译字典。你必须能够证明自己需要使用字典，通常提供出生证明或者护照就可以解决这个问题。

学习和备考要领

在 CISSP 考试的准备过程中，我们建议安排一个月左右的时间进行学习或者每晚进行强化学习。下面提供了几个建议，能够帮助你充分地利用学习时间，你也可以根据自己的学习习惯进行一些调整：

- 每一章的内容要花一两个晚上阅读并进行复习。
- 完成本书与配书光盘上提供的所有考试练习。完成每章的书面练习与自测题，这有助于你明确需要通过认真学习和花费时间才能掌握的关键概念与策略。
- 从 Web 站点 www.isc2.org 上查阅$(ISC)^2$的学习教程。
- 使用随书光盘上的闪视卡强化对概念的理解。

我们建议读者将一半的学习时间用于阅读和复习各种概念，另一半时间则用于完成考试练习。学生们反映：投入考试练习的时间越多，就更容易记住考点。此外，你还需要经常访问诸如 www.cccure.org 和 www.cissp.com 之类的资源站点以及其他关注 CISSP 的 Web 站点。

认证过程的完成

一旦接到成功通过 CISSP 认证的通知，你还剩下最后一个步骤就能够真正获得 CISSP 认证资格。这个最后步骤被称为书面证明(endorsement)。从根本上说，这需要某个熟悉你工作经历的人为你签字并提交书面证明文件。书面证明文件会作为通知你已经通过认证考试的电子邮件的附件发送给你。你只需将书面证明文件和自己的履历发送给某位声誉良好的 CISSP 即可。证明人必须查看你的履历，确认你在 10 个 CISSP 领域具有足够的从业经历，随后他会通过传真或邮寄方式向$(ISC)^2$提交有自己签名的证明文件。在接到考试通过确认邮件之后，你必须在 90 天之内向$(ISC)^2$提交书面证明文件。一旦$(ISC)^2$收到已签名的书面证明文件，认证过程就会结束，并且会给你邮寄一个欢迎成为 CISSP 的包裹。

如果很遗憾未通过考试，那么你还可以在最短的时间内参加第 2 次考试。不过，参加第 2 次考试应当准备得更加充分。如果再次失手，那么$(ISC)^2$会要求你在等待 6 个月后才能参加第 3 次考试。

CISSP 的继续认证

$(ISC)^2$提供了 3 种继续认证，这些认证只针对具有 CISSP 认证资格的人员。在 3 个继续认证中，$(ISC)^2$应用 CISSP 考试所涉及的概念并侧重于特定的领域，也就是体系结构、管理和工程。下面讲述了这三种认证：

- **信息系统安全体系结构专家(Information Systems Security Architecture Professional，ISSAP)认证**：针对从事信息安全体系结构工作的人员。这个认证涉及的主要领域包括：访问控制系统和方法学；密码术；物理安全集成；需求分析和安全规范、指导原则与标准；业务连续性计划和灾难恢复计划的技术方面；以及电信和网络安全。ISSAP 既可以为设计安全系统或基础架构的人员提供认证，也可以为审计和分析这些安全体系结构的人员提供认证。
- **信息系统安全管理专家(Information Systems Security Management Professional，ISSMP)认证**：针对管理信息安全策略、实践、准则与过程的人员。这个认证涉及的主要领域包括：企业安全管理实践；整个企业的系统开发安全性；法律、犯罪调查、法庭辩论与道德规范；监督操作安全合规性；理解业务连续性计划、灾难恢复计划以及操作计划的连续性。ISSMP 为负责管理安全基础架构的专业人员提供认证。
- **信息系统安全工程专家(Information Systems Security Engineering Professional ISSEP)认证**：针对安全硬件和软件信息系统、组件或应用程序的设计与工程人员。这个认证涉及的主要领域包括：认证和鉴定；系统安全工程；技术管理；美国政府信息保障规则和规章制度。绝大多数 ISSEP 为美国政府或某个管理政府安全检查的政府承包商工作。

要了解这些继续认证的更多信息，请访问$(ISC)^2$的 Web 站点 www.isc2.org。

本书的组织结构

本书涵盖了 CISSP 公共知识体系(Common Body of Knowledge，CBK)的 10 个领域，并且对每个领域都进行了深入充分的讨论，从而使你能够清楚地理解这些内容。本书的主体由 19 个章节组成。前 9 个领域分别包含在两章中，最后一个领域(也就是物理安全)则涵盖在第 19 章中。下面列出了各领域所对应的章节：

第 1 章和第 2 章 访问控制
第 3 章和第 4 章 通信和网络安全
第 5 章和第 6 章 信息安全与风险管理
第 7 章和第 8 章 应用安全
第 9 章和第 10 章 密码术
第 11 章和第 12 章 安全体系结构与设计
第 13 章和第 14 章 操作安全
第 15 章和第 16 章 业务连续性与灾难恢复计划
第 17 章和第 18 章 法律、合规性与调查
第 19 章 物理(环境)安全

每章包含的一些要素都有助于你强化学习重点和测试掌握知识的程度，接下来我们将详细介绍这些要素。

本书的要素

阅读本书时，你会发现许多重复出现的要素。下面描述了其中一些要素：

- **关键术语与术语表**：在每一章中，我们都会明确给出关键术语(key term)，你必须掌握这些重要的术语。此外，在本书的术语表中也可以找到这些术语及其定义。
- **小结**：小结简要回顾了每一章所涵盖的内容。
- **应试要点**：应试要点所指出的要点会在或曾经在 CISSP 考试中以某种形式出现。虽然我们不可能知道某次考试中会出现哪些考点，但是这个部分强化了重要的概念，这对于你理解知识领域以及 CISSP 考试的范围十分重要。
- **复习题**：每章都包含一些练习题，这些练习题被用来测试你对相应章节所讲述知识的掌握程度。阅读每章之后，请完成练习题。如果不能正确回答某些问题，那么就表明你需要重新学习相关的知识。每章的最后都会给出练习题的答案。
- **书面练习**：每章都包含综合了相应章节的各种概念与主题的书面练习。这些问题的意图是帮助你将零散知识点综合在一起，从而建议或描述潜在的安全策略或解决方案。
- **真实场景**：在每一章中，至少存在两个典型的、贴近现实的工作环境描述，如果理解了相应章节内容涉及的安全策略和方法，将能够解决现实问题或避开潜在的困难。通过对真实场景的学习，你能够掌握在真实工作环境中应当如何应用具体的安全策略、指导原则或惯例。

配书光盘的内容

经过努力，我们找到了一些有助于通过认证的必要工具。准备 CISSP 考试时，你应当安装下面要介绍的这些工具。

Sybex 公司提供的备考软件

Sybex 公司专家编制的备考软件能够帮助你准备 CISSP 考试。在这个考试引擎中，你会找到本书中的所有复习题和评估题。此外，光盘上还会专门给出 5 个额外的考试。你可以进行评估测试，可以逐章进行测试，可以进行模拟考试，也可以完成包括所有问题的随机考试。

适用于 PC 和 Palm 掌上设备的电子闪视卡

Sybex 公司的电子闪视卡包括数百个问题，其目的是进一步考验你对 CISSP 考试的准备程度。借助于复习题、模拟考试以及闪视卡，你将积累足够多的应试经验！

PDF 格式的电子书

在配书光盘中，Sybex 公司提供了 PDF 格式的电子书，从而使你能够在 PC 或便携式电脑上阅读该书。如果出门在外不想带书，或者愿意在计算机上阅读，那么光盘就能够提供这样的便利。此外，配书光盘上还带有 Adobe Acrobat 软件。

额外考试

在配书光盘中，Sybex 公司提供了 5 个额外考试，每个考试都用于考察你对 CISSP CBK 中要点的理解。

如何使用本书及配书光盘

本书设计了许多能够指导你准备 CISSP 认证考试的细节。每章开头都会开宗明义地列出相应章节将会详细讨论的 CISSP 知识点，每章结尾都提供了许多练习题，配书光盘上的模拟考试能够帮助你测试对各种知识的记忆以及发现自己需要继续学习的内容。下面给出了一些使用本书与光盘的建议：

- 阅读本书前先完成评估测试。这样你会了解自己需要多花些时间学习的内容以及只需快速浏览的内容。
- 阅读完每章后，完成相应章节的复习题。如果答案出错，就重新阅读本章的相关内容并分析相应的主题，在需要了解更多信息时还可以利用其他资源。
- 将闪视卡下载至手持设备，每天抽空进行复习。
- 利用一切机会进行自测。除了评估测试和复习题之外，配书光盘上还有额外的考试。在不查阅本书的情况下完成这些额外考试，根据考试结果复习还未掌握的知识，直至能够完全理解和应用相关概念为止。

最后，尽可能找到学习伙伴。与他人一起学习和参加考试，这会使认证考试过程更为

愉快，并且在遇到难以理解之处可以寻求伙伴的帮助。此外，通过帮助别人克服学习障碍，你也可以巩固自己的知识。

评估测试

1. Which of the following type of access control seeks to discover evidence of unwanted, unauthorized, or illicit behavior or activity?
   A. Preventive　　B. Deterrent
   C. Detective　　D. Corrective
2. Can you define and detail the aspects of password selection that distinguish good password choices from ultimately poor password choices?
   A. Difficult to guess or unpredictable
   B. Meet minimum length requirements
   C. Meet specific complexity requirements
   D. All of the above
3. Which of the following is most likely to detect DoS attacks?
   A. Host-based IDS　　B. Network-based IDS
   C. Vulnerability scanner　　D. Penetration testing
4. Which of the following is considered a denial-of-service attack?
   A. Pretending to be a technical manager over the phone and asking a receptionist to change their password
   B. While surfing the Web, sending to a web server a malformed URL that causes the system to use 100 percent of the CPU to process an endless loop
   C. Intercepting network traffic by copying the packets as they pass through a specific subnet
   D. Sending message packets to a recipient who did not request them simply to be annoying
5. At which layer of the OSI model does a router operate?
   A. Network layer　　B. Layer 1
   C. Transport layer　　D. Layer 5
6. Which type of firewall automatically adjusts its filtering rules based on the content of the traffic of existing sessions?
   A. Static packet filtering　　B. Application-level gateway
   C. Stateful inspection　　D. Dynamic packet filtering
7. A VPN can be established over which of the following?
   A. Wireless LAN connection　　B. Remote access dial-up connection
   C. WAN link　　D. All of the above

8. Email is the most common delivery vehicle for which of the following?
   A. Viruses　　B. Worms
   C. Malicious code　　D. All of the above
9. The CIA Triad is comprised of what elements?
   A. Contiguousness, interoperable, arranged
   B. Authentication, authorization, accountability
   C. Capable, available, integral
   D. Availability, confidentiality, integrity
10. Which of the following is not a required component in the support of accountability?
   A. Auditing　　B. Privacy
   C. Authentication　　D. Authorization
11. Which of the following is not a defense against collusion?
   A. Separation of duties　　B. Restricted job responsibilities
   C. Group user accounts　　D. Job rotation
12. A data custodian is responsible for securing resources after _____ has assigned the resource a security label.
   A. senior management　　B. data owner
   C. auditor　　D. Security staff
13. In what phase of the Capability Maturity Model for Software (SW-CMM) are quantitative measures utilized to gain a detailed understanding of the software development process?
   A. Repeatable　　B. Defined
   C. Managed　　D. Optimizing
14. Which one of the following is a layer of the ring protection scheme that is not normally implemented in practice?
   A. Layer 0　　B. Layer 1
   C. Layer 3　　D. Layer 4
15. What is the last phase of the TCP/IP three-way handshake sequence?
   A. SYN packet　　B. ACK packet
   C. NAK packet　　D. SYN/ACK packet
16. Which one of the following vulnerabilities would best be countered by adequate parameter checking?
   A. Time-of-check-to-time-of-use　　B. Buffer overflow
   C. SYN flood　　D. Distributed denial of service
17. What is the value of the logical operation shown here?
   X:　　0 1 1 0 1 0
   Y:　　0 0 1 1 0 1
   X ⊕ Y:　　?
   A. 0 1 1 1 1 1　　B. 0 1 1 0 1 0

C. 0 0 1 0 0 0　　D. 0 0 1 1 0 1

18. In what type of cipher are the letters of the plain-text message rearranged to form the cipher text?
    A. Substitution cipher　　B. Block cipher
    C. Transposition cipher　　D. One-time pad
19. What is the length of a message digest produced by the MD5 algorithm?
    A. 64 bits　　B. 128 bits
    C. 256 bits　　D. 384 bits
20. If Renee receives a digitally signed message from Mike, what key does she use to verify that the message truly came from Mike?
    A. Renee's public key　　B. Renee's private key
    C. Mike's public key　　D. Mike's private key
21. Which of the following statements is true?
    A. The less complex a system, the more vulnerabilities it has.
    B. The more complex a system, the less assurance it provides.
    C. The less complex a system, the less trust it provides.
    D. The more complex a system, the less attack surface it generates.
22. Ring 0, from the design architecture security mechanism known as protection rings, can also be referred to as all but which of the following:
    A. privileged mode　　B. supervisory mode
    C. system mode　　D. user mode
23. Which of the following is not a composition theory related to security models?
    A. Cascading　　B. Feedback
    C. Iterative　　D. Hookup
24. Which level of Trusted Computer System Security Criteria (TCSEC) required that the evaluated system have mandatory access controls?
    A. C2　　B. B1
    C. D　　D. C1
25. Audit trails, logs, CCTV, intrusion detection systems, antivirus software, penetration testing, password crackers, performance monitoring, and cyclic redundancy checks (CRCs) are examples of what?
    A. Directive controls　　B. Preventive controls
    C. Detective controls　　D. Corrective controls
26. System architecture, system integrity, covert channel analysis, trusted facility management and trusted recovery are elements of what security criteria?
    A. Quality assurance　　B. Operational assurance
    C. Life cycle assurance　　D. Quantity assurance

27. Which of the following is a procedure designed to test and perhaps bypass a system's security controls?
A. Logging usage data
B. War dialing
C. Penetration testing
D. Deploying secured desktop workstations

28. Auditing is a required factor to sustain and enforce what?
A. Accountability
B. Confidentiality
C. Accessibility
D. Redundancy

29. What is the formula used to compute the ALE?
A. ALE = AV * EF
B. ALE = ARO * EF
C. ALE = AV * ARO
D. ALE = EF * ARO

30. What is the first step of the business impact assessment process?
A. Identification of priorities
B. Likelihood assessment
C. Risk identification
D. Resource prioritization

31. Which of the following represent natural events that can pose a threat or risk to an organization?
A. Earthquake
B. Flood
C. Tornado
D. All of the above

32. What kind of recovery facility enables an organization to resume operations as quickly as possible, if not immediately upon failure of the primary facility?
A. Hot site
B. Warm site
C. Cold site
D. All of the above

33. What law allows ISPs to voluntarily provide government investigators with a large range of user information without a warrant?
A. Electronic Communications Privacy Act
B. Gramm-Leach-Bliley Act
C. USA PATRIOT Act
D. Privacy Act of 1974

34. In the United States, how are the administrative determinations of federal agencies promulgated?
A. Code of Federal Regulations
B. United States Code
C. Supreme Court decisions
D. Administrative declarations

35. Why are military and intelligence attacks among the most serious computer crimes?
A. The use of information obtained can have far-reaching detrimental strategic effect on national interests in an enemy's hands.
B. Military information is stored on secure machines, so a successful attack can be embarrassing.
C. The long-term political use of classified information can impact a country's

leadership.

D. The military and intelligence agencies have ensured that the laws protecting their information are the most severe.

36. What type of detected incident allows the most time for an investigation?

A. Compromise
B. Denial of service
C. Malicious code
D. Scanning

37. If you want to restrict access to one direction within a facility, which would you choose?

A. Gate
B. Turnstile
C. Fence
D. Mantrap

38. What is the point of a secondary verification system?

A. To verify the identity of a user
B. To verify the activities of a user
C. To verify the completeness of a system
D. To verify the correctness of a system

评估测试答案

1. C。检测性访问控制用于发现(和记录)不受欢迎的或未授权的活动。更多的信息，请参看第 1 章。
2. D。强密码难以猜测、不可预测而且长度不低于下限，这能够确保无法计算得到明确的密码数据。强密码可以随机生成，而且可以使用所有字母、数字和标点字符；一定不要写下和共享密码；不能存储在公共可访问的或普遍可读的位置；一定不能以明文形式发送。更多的信息，请参看第 1 章。
3. B。网络型 IDS 通常能够检测攻击的开始或者正在进行的攻击尝试(包括 DoS)，不过不能提供攻击是否成功的信息，也不能确定被攻击的系统、用户账户、文件或者应用程序。主机型 IDS 检测和跟踪 DoS 攻击有一定难度。脆弱性扫描程序无法检测 DoS 攻击，它只能用于测试可能存在的脆弱性。渗透测试可以引发 DoS 或测试 DoS 脆弱性，但是它并非一种检测工具。更多的信息，请参看第 2 章。
4. B。并非所有 DoS 事件都会导致恶意攻击。操作系统代码、服务和应用程序中的错误都能成为 DoS 的条件。有关这种情况的例子包括：进程无法释放对 CPU 的控制，或者某个服务所占用的系统资源超出了该服务请求的范围。社会工程与嗅探技术通常不针对 DoS 攻击。更多的信息，请参看第 2 章。
5. A。网络硬件设备(包括路由器)工作在第 3 层，也就是网络层。更多的信息，请参阅第 3 章。
6. D。动态包过滤防火墙支持实时更改基于通信内容的过滤规则。更多的信息，请参看第 3 章。
7. D。VPN 链接可以建立在任何其他的网络通信连接上。这些网络通信连接可以是典

型的 LAN 线缆连接、无线 LAN 连接、远程访问拨号连接或 WAN 连接，甚至还可以是用户访问公司 LAN 所使用的 Internet 连接。更多的信息，请参看第 4 章。

8. D。电子邮件是病毒、蠕虫、特洛伊木马、破坏性宏文件以及其他恶意代码的最常用传输手段。更多的信息，请参看第 4 章。

9. D。CIA 安全三原则(CIA Triad)的组成部分是机密性、可用性与完整性。更多的信息，请参看第 5 章。

10. B。隐私不是提供可问责性的必要组件。更多的信息，请参看第 5 章。

11. C。组用户账户允许多个人在一个用户账户下工作。这种情况允许共谋(因为阻止个人可问责性)。更多的信息，请参看第 6 章。

12. B。只有在数据所有人为资源分配安全标签之后，数据管理人才可能适当地保护资源的安全。更多的信息，请参看第 6 章。

13. C。SW-CMM 的管理阶段涉及量化开发标准的使用。软件工程研究所(Software Engineering Institute，SEI)为这一级定义了主要处理区域(量化处理管理和软件质量管理)。更多的信息，请参看第 7 章。

14. B。第 1 层和第 2 层包含设备驱动程序，但是实际上通常没有执行。第 0 层包含安全内核。第 3 层包含用户应用程序。第 4 层并不存在。更多的信息，请参看第 7 章。

15. B。首先将 SYN 数据包从初始主机发送到目标主机。接着，目标主机利用 SYN/ACK 数据包进行响应。初始主机发送 ACK 数据包，随后连接建立。更多的信息，请参看第 8 章。

16. B。参数检查被用于防止缓冲区溢出攻击的可能性。更多的信息，请参看第 8 章。

17. A。符号 ⊕ 代表或 OR 操作，当一个或两个输入比特为真时，结果就为真。更多的信息，请参看第 9 章。

18. C。换位密码使用某种加密算法重新安排明文消息的字母，从而形成密文消息。更多的信息，请参看第 9 章。

19. B。MD5 算法为任意的输入内容生成一个 128 比特消息摘要。更多的信息，请参看第 10 章。

20. C。所有接收方都可以使用 Mike 的公钥对数字签名进行身份验证。更多的信息，请参看第 10 章。

21. B。系统越复杂，所提供的安全保证越少。更高的复杂度意味着更多方面存在脆弱性以及必须在更多方面防范威胁。更多的脆弱性与更多的威胁意味着系统随之提供的安全性可靠程度越低。更多的信息，请参看第 11 章。

22. D。Ring 0 级别直接访问大多数资源，由于用户模式要求限制对资源的访问，所以该模式并非适当的标签。更多的信息，请参看第 11 章。

23. C。迭代不属于与安全模型相关的构成理论。级联、反馈和挂接才是与安全模型相关的三个构成理论。更多的信息，请参看第 12 章。

24. B。B1 级是要求强制访问控制(mandatory access control，MAC)的级别。其他要求强制访问控制的级别是 B2、B3 和 A1。D、C1 和 C2 不要求 MAC。更多的信息，请参看第 12 章。